ABSTRACT

This invention relates to a method for generating a shared secret value between entities in a data communication system, one or more of the entities having a plurality of members for participation in the communication system, each member having a long term private key and a corresponding long term public key. The method comprises the steps of generating a short term private and a corresponding short term public key for each of the members; exchanging short term public keys of the members within an entity. For each member then computing an intra-entity shared key by mathematically combining the short term public keys of each the members computing an intra-entity public key by mathematically combining its short-term private key, the long term private key and the intra-entity shared key. Next, each entity combines intra-entity public keys to derive a group short-term S_i public key; each entity transmitting its intra-entity shared key and its group short term public key to the other entities; and each entity computing a common shared key K by combining its group short term public key (S_i), with the intra-entity shared key ($\overline{X}_i$), and a group short term public ($\overline{S}_i$) key received from the other entities.